基于椭圆曲线的 RFID 协议的安全分析①

蒋德山，陈志德，陈金梁

(福建师范大学 数学与计算机科学学院，福州 350007)

摘 要: Matinez 等人已经提出了一种只依赖于椭圆曲线密码和零知识认证模式的无线射频认证协议. 本文中，我们指出该协议不能抵抗去同步化攻击. 攻击者只需拦截最后服务器发给标签的确认消息，就会导致后台服务器和标签存储的共享秘钥不一致. 对此，我们提出了修正方案，并证明了修订后的协议可以抵抗去同步化攻击.

关键词: Web 信息提取；知识表示；数据密集型 Web 页面；基于本体的关键词库

Secure Analysis of Elliptic Curve Based on RFID Protocol

JIANG De-Shan, CHEN Zhi-De, CHEN Jin-Liang

(School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China)

Abstract: Matinez et al has proposed a secure RFID protocol which only relies on the use of Elliptic Curve Cryptography and a zero knowledge based authentication scheme. In this paper, we present that the proposed protocol can't resist desynchronization attack. The attacker only block the last acknowledge message from Back End Server. Then the share key of Tag and Back End Server is different. For this, we propose our revised scheme, and prove that revised scheme can resist desynchronization attack.

Key words: RFID; authentication protocol; ECC; desynchronization attack

1 概述

条形码标签被应用于实际已经很长时间了. 虽然使用它们的代价比较小，但是对于某些需要更多隐私和信息保护的应用，它们却不能提供充足的安全性. 另一个缺点是条形码标签必须在一个可视接触的距离才能被一个光学阅读器访问. 这些缺陷大大的限制了它们的应用范围. 随后，研究人员开发了无线射频认证来识别特殊的物体，在阅读器和标签之间利用无线信号进行无需物理接触的数据传输. 无线射频认证系统的其他优点是：阅读器可以同时访问多个标签，标签可以快速且容易地被阅读器访问，标签可以重复使用并且有高数据存储能力. 由于具有上述优点，无线射频认证系统被广泛应用于很多领域. 其中一些常见的应用：电子收费，珍稀野生动物追踪，电子护照，医疗应用，资产管理，运输和物流管理.

无线射频认证是一种利用无线电信号来鉴别物体的无线自动认证和数据捕获技术(简称 WAIDST)[1]. 由于无线射频认证系统中的标签在电路（即计算能力）、存储能力和电源消耗方面都存在限制，所以设计一个有效率而且安全的无线射频认证协议具有很大的挑战. 一个成熟的无线射频识别协议必须可以抵抗已知的隐私和安全威胁，例如标签信息泄露、标签位置追踪、重放攻击、拒绝服务攻击和伪造攻击[2]. 对于无线射频认证协议，以下的安全性质是在协议的设计和分析过程中应该着重考虑的部分[3].

相互认证：标签和服务器应该在互相认证后才能通信. 标签到服务器的认证使得服务器可以确定一个当前通信的标签是合法的. 服务器到标签的认证使得标签可以确信与它正在通信的服务器是已经授权的[4]; 不可追踪性：这种性质从直观概念上来看是攻击者无

① 基金项目：国家自然科学基金(61072080);福建省 2013 年战略性新兴产业技术开发项目([2013]266);
福建省高校产学合作科技重大项目(2011H6008);福建省自然科学基金(2012J01252)

收稿时间:2013-09-16;收到修改稿时间:2013-10-14

法区分它两次发现的是否为同一个标签，这种性质就是不可追踪[5];抗失调性：如果一个标签总能被服务器认证成功，那么这个协议是抗失调的[6]. 这种性质确保了在协议执行的过程中，任何一个标签都不会陷入一种没有服务器可以认证它的状态. 在去同步化(即失调)攻击中，攻击者会试图破坏共享密钥或身份证明的更新，使得标签和服务器中存储的共享密钥不同，致使以后的认证都不能成功.

文献[7-10]提出无线射频认证系统安全问题的理论模型. 在文献[8]的理论框架中，攻击者被分为两大类：广泛的(或有限的)和强壮的(或虚弱的)攻击者. 广泛的攻击者拥有获得来自服务器认证的结果(接受或是拒绝). 假如攻击者能够抽取出加密消息的密码并且重用它，那么这个攻击者就是强壮的. 否则，他就是虚弱的攻击者. 假如某个协议可以抵抗广泛的而且强壮的攻击者的攻击，这个协议就是广泛的而且强壮的安全协议.

大多数的无线射频认证协议都关注于对称密钥加密或是哈希加密函数，通常觉得公钥密码算法的计算很耗时间，它们对于如此低成本的应用环境是很复杂的. 在文献[11]中，作者们已经显示了椭圆曲线密码也适合于在无线射频认证系统安全协议中应用. 他们设计了一个基于椭圆曲线密码的处理器并把它应用在无线射频认证标签. 在文献[12-14]中，作者们提出其他的椭圆曲线密码处理器. 文献[15]将椭圆曲线密码和零知识认证模式结合. 他们证明了所提出的协议具有前向安全性. 然而，在本文中我们将显示出这个认证协议在一个广泛的-虚弱的攻击者的攻击下不能够抵抗去同步化攻击的弱点.

全文结构如下：第 2 部分我们将介绍系统模型和攻击模型；文献[15]提出的协议将在第三部分详细介绍；我们在第四部分进行安全性分析（即攻击）；在第 5 部分给出可以抵抗去同步化攻击的修订方案；最后在第 6 部分对全文做出总结.

2 系统背景

2.1 系统模型

一个典型的无线射频认证系统由三个主要部分组成：标签，阅读器和后台服务器(如图 1). 标签一般根据它是否有电池被分为消极的和积极的. 积极的标签有自己的能量资源，所以它有很高的处理信息的能力和广泛的传播范围. 相反地，消极的标签在计算能力和传播范围上都有自身的限制. 近年来，消极的标签普遍应用于无线射频认证系统，它们扮演着主要的角色，因此本文所要讨论的标签是基于消极低能耗的.

阅读器给标签发送一个无线信号并监听标签的响应(如图 2 所示). 该标签收到这个信号后就回复自己的唯一身份信息. 阅读器把收到的身份信息传送给后台服务器，后台服务器经核实后才能认证该标签. 在这个过程中，阅读器和标签之间的通信具有以下的特点：

① 标签发给阅读器的唯一身份信息是通过无线电频率通信而且未经任何处理.

② 当有来自阅读器的查询消息时，标签才会发送自己的唯一身份信息.

③ 后台服务器和阅读器之间的通信是安全的. 阅读器和标签之间的通信是不安全的，因为它们使用无线电频率通信.

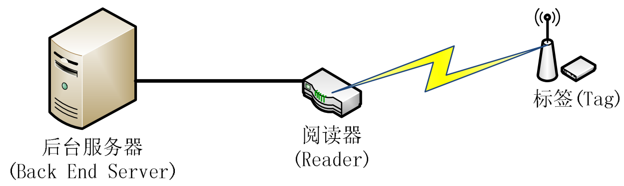


图 1 无线射频识别系统结构图

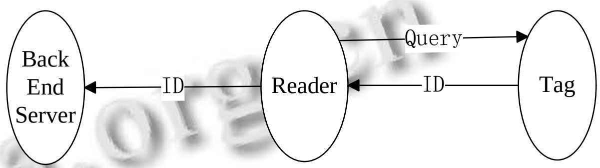


图 2 无线射频识别系统逻辑图

2.2 威胁模型

以上的各种特性可以导致无线射频认证系统出现严重的信息泄露和各种安全隐患，并且攻击者可以将已获得的信息应用在各种非法的应用上. 以下内容和表 1 是攻击者从无线射频认证系统获得信息的一个攻击模型的定义.

① 监听

由于标签和阅读器之间的通信是基于无线射频的，所以每个人都能够监听. 攻击者可以通过监听获得通信消息或者是利用监听到的消息开始另一个攻击.

② 暴力攻击

暴力攻击是一种可以分析认证协议的秘密消息的

攻击方法. 它获得在标签和阅读器通信时窃听到的消息, 分析这些消息, 然后攻击者便可以获得连接标签和拥有者的身份信息.

③ 定位追踪

攻击者使用一个恶意的阅读器能够获得标签的唯一身份信息而且还能够发现这个标签属于哪个用户. 为了完成这样一个攻击, 攻击者需要不间断地向被追踪的标签发送询问消息. 由于标签中包含的信息与相关的物体往往是关联性很强的. 所以通过这种方法, 标签的持有者的位置信息便会暴露而且他的隐私也被入侵.

④ 用户隐私问题

攻击者分析一个特定的标签的输出来获得它所关联的物体的信息, 这些信息可以用来入侵持有者的隐私.

⑤ 定位隐私问题

由于标签的输出是不变或是有规律的变化的, 所以追踪标签便可以追踪持有者.

⑥ 重放攻击

这种攻击就是攻击者把之前阅读器和标签通信的消息再次用于通信, 并且获得认证.

⑦ 中间人攻击

这种攻击类似于重放攻击. 但是与之不同的是, 攻击者再一次发送的消息是经过自己修改的, 而且这种修改能够被认证.

⑧ 物理攻击

标签有一个致命的缺点, 这个缺点使它易受物理攻击. 在确切掌握了一个标签的信息之后, 攻击者便可以伪造或是改造它.

表 1　威胁与安全需要

攻击类型	问题描述	安全需要
监听	用户隐私和位置隐私问题	保密性
暴力攻击		
位置跟踪		不可区分性和前向安全
重放攻击	伪造问题	相互认证
中间人攻击		
物理攻击		

3　基于椭圆曲线密码的安全认证协议

3.1 符号

本篇文章用到的符号罗列如下:

表 2　本文所用符号

符号	描述
F_q	有限域
E/F_q	有限域内的椭圆曲线
$Q \in E(F_q)$	基于子群的生成器
$P \in <Q>$	阅读器的公钥
$LB(.)$	输出左面部分
$MB(.)$	输出中间部分
$s \in [2, g-1]$	阅读器的密钥
r	阅读器产生的随机数
c	标签产生的随机数
K_j^i	第 i 个标签的第 j 次秘密椭圆曲线点
$x(K_i^i), y(K_{i-}^i$	分别是当前的横坐标秘密点和之前的纵坐标秘密点

3.2 协议描述

文献[15]介绍的协议的详细流程如图 3. 这个协议主要由四个部分组成: 启动阶段, 阅读器认证阶段, 标签认证阶段, 标签核实阶段, 详细介绍如下:

(1) 启动阶段

在这个阶段, 协议所需的私钥和公钥已经产生. $K_1^i \in E(F_q)$ 是第 i 个标签的初始密码点. 一个有限域 F_q 和在该有限域上的椭圆曲线 E/F_q. s 被选作阅读器的私钥. 阅读器的公钥 P=sQ.

(2) 阅读器认证阶段

①阅读器产生一个随机数 r, 并且计算 W=rQ. 然后阅读器 R 将 W 发送给标签 T.

②收到了阅读器 R 的消息后, 标签 T 选择自己的随机数 c 回复给 R.

③收到了标签 T 的回复后, 阅读器 R 计算 a=r+cs, 然后发给 T.

④收到阅读器 R 的消息 a 后, 标签 T 可以核实等式 aQ-cP=W 是否成立, 从而判断阅读器 R 的合法性.

(3) 标签认证阶段

当标签成功核实等式 aQ-cP=W 后, T 计算伪身份 $id_j^i = LB(K_j^i) * LB(y(K_{j-1}^i))$ 和 $K_{j+1}^i = zQ(z = f(x(K_j^i)))$ 下一个密码点. 然后标签 T 存储 K_{j+1}^i 并且把它的伪身

份 id^i_j 发给阅读器 R.

(4) 标签核实阶段

收到标签 T 的伪身份 id^i_j，阅读器 R 将 id^i_j 传给后台服务器 S. 当后台服务器 S 收到 id^i_j 后，它首先检查消息是否有效. 如果有效，S 将会计算出 K^i_{j+1} 并且计算 $ack^i_j = MB(x(K^i_j)) * MB(x(K^i_{j+1}))$. 然后 S 发送 ack^i_j 给阅读器 R 并且更新共享密钥 $K^i_{j-1} = K^i_j and K^i_j = K^i_{j+1}$. 然后将 R 这个确认信息 ack^i_j 继续传送给标签 T. 最后标签 T 核实收到的确认信息是否有效. 当且仅当 ack^i_j 有效时，标签 T 更新自己的共享密钥.

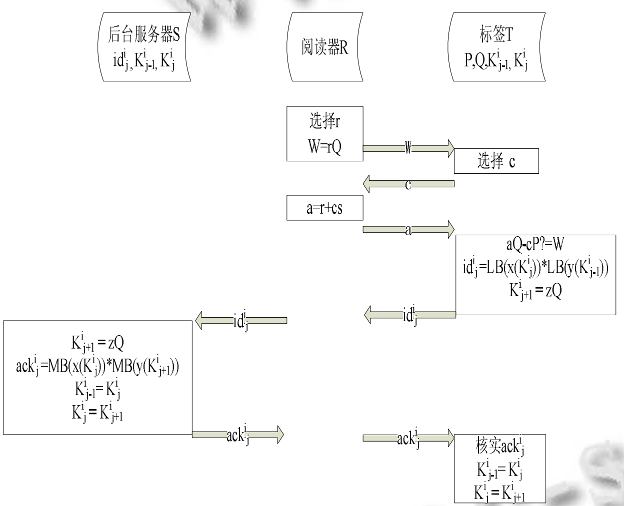


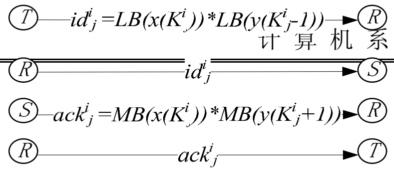
图 3 基于椭圆曲线密码和零知识认证的安全协议

4 协议的安全性分析

根据以上的描述，该协议自身仍然存在一定的缺陷，原协议无法抵抗以下的攻击类型.

(1) 会陷入去同步化攻击，导致正常的标签无法获得认证

标签 T 的认证和更新阶段：当阅读器 R 认证成功后，标签 T 将会向后台服务器 S 发送伪 ID. 具体描述如下:

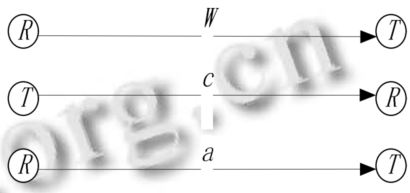


由于服务器 S 和标签 T 都只保存了一份的共享密钥 K^i_{j-1}, K^i_j，假如攻击者将服务器回应的消息 ack^i_j 拦截，那么没有收到确认消息的标签 T 仍保存原共享密钥，而服务器 S 已经更新了共享密钥，在之后的通信中，标签和服务器保存的共享密钥将不同步，即该标签无法被认证. 这样去同步化攻击完成，因为这个标签将不能和任何一个阅读器正常通信.

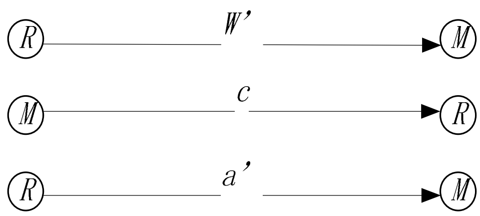
(2) 会陷入伪造攻击，导致攻击者可以利用询问获得的伪 ID 伪造标签

若攻击者监听与标签通信并且获得了他的伪 ID，那么便可以伪造标签的身份与服务器通信. 原协议虽然需要首先通过 $aQ - cP = 0$ 验证阅读器的合法身份，但是由于原协议中的阅读器发给标签的消息 $a = r + cs$ 没有将数据完全随机化，攻击者只需要监听一次合法标签和阅读器的通信，再模仿一次标签与阅读器通信，将这两次的消息叠加便可以模仿阅读器访问标签，并且可以得到合法认证，获得标签的伪 ID. 获得标签的伪 ID 后，攻击者就可以模仿合法标签访问服务器. 具体攻击步骤如下(假设 M 为攻击者):

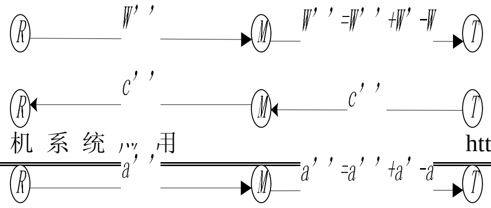
①监听



②模仿标签



③模仿阅读器并监听伪 ID



因为 $W''=W''+W-W=(r''+r'-r)Q$ $a''=a''+a'-a=r''+r'-r+c''s$，所以在标签收到 a'' 后：

$a''Q-c''P=(r''+r'-r+c''s)Q-c''sQ=(r''+r'-r)Q=W''$，攻击者获得认证成功，标签下一步发送自己的伪 ID，攻击者就可以获得标签的伪 ID.

5 修改后的协议

5.1 新协议描述

改进后的协议的详细流程如图 4 所示. 新协议中服务器和标签都保存了 2 份的共享秘钥.

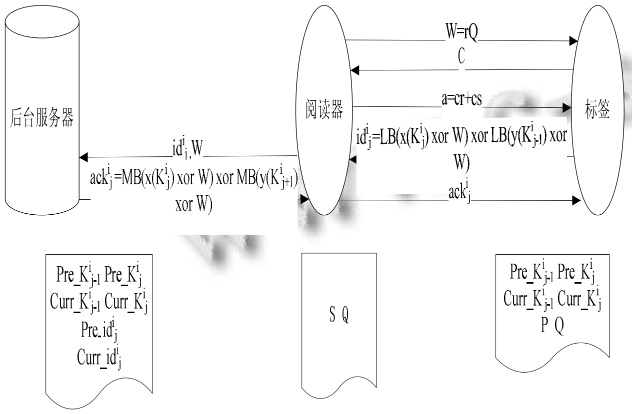


图 4 修改后的协议

5.2 认证过程

(1)阅读器选择随机数 r，计算证据 $W=rQ$ 并发送给标签

(2)标签选择自己的随机数 C 发送给阅读器

(3)阅读器计算 $a=cr+cs$ 发送给标签

(4)标签验证 $aQ-cP=0$ 后，计算

$$\mathrm{Curr\_id}^i_j=LB(x(Curr\_K^i_j)\ xor\ W)\ xor\ LB(y(Curr\_K^i_{j-1})\ \mathrm{xor}\ W)$$

发送给阅读器，

如果之后没有收到确认信息，继续发送

$$\mathrm{Pre\_id}^i_j=LB(x(\mathrm{Pr}e\_K^i_j)\ xor\ W)\ xor\ LB(y(\mathrm{Pr}e\_K^i_{j-1})\ \mathrm{xor}\ W)$$

(5)阅读器发送 $Curr\_id^i_j, W$ 给服务器

(6)服务器验证 $Curr\_id^i_j$，若匹配成功就计算 ack^i_j 发送给阅读器，如果匹配不成功协议执行结束，返回第(4)步

(7)阅读器 ack^i_j 发送给标签

5.3 安全性分析

修改后的协议能够保持原协议的诸多优点，如保证内容隐私、防止追踪攻击的同时，又进一步客服了原协议的不足. 对其安全性分析如下：

(1) 抵抗伪造攻击

在该协议中，伪 ID 的生成式中加入了 W，这样使得标签发给服务器的伪 ID 也会随着阅读器产生的随机数的变化而变化，使得攻击者不能进行伪造攻击，重新发送之前监听到的伪 ID 给阅读器，在服务器端不会得到认证，因为 $r'\neq r$.

(2) 抵抗去同步化攻击

在该协议中，同时在标签和服务器保存了 2 份共享密钥

$$\mathrm{Pr}e\_K^i_{j-1},\mathrm{Pr}e\_K^i_j,Curr\_K^i_{j-1},Curr\_K^i_j$$

若标签发送给服务器的 $Curr\_id^i_j$ 没有得到认证，标签还可以再一次发送消息 $\mathrm{Pr}e\_id^i_j$，服务器保存了 2 份的共享密钥，总有一份会得到认证，攻击者不能只拦截一次就实现去同步化攻击.

由以上分析可知，修改后的协议摒弃了原有协议的缺陷，即通过抵抗去同步化攻击，使得标签能够成功被认证，同时又通过伪 ID 的完全随机化，使得攻击者无法进行伪造攻击. 安全性得到很大提高.

6 结语

本文介绍了一种基于椭圆曲线密码的 RFID 安全协议，发现其不能抵抗去同步化攻击的安全漏洞. 我们通过在服务器和标签都存储了两份的共享密钥来使协议能够抵抗去同步化攻击. 进而完全随机化阅读器发出的证据，修改后的协议也能够抵抗伪造攻击. 通过对其进行安全性分析可知，该协议可以保证内容隐私，抵抗伪造攻击，抵抗去同步化攻击. 但是，修改后的协议在服务器端采用遍历搜索的认证方式，这种低

效率的搜索不适合用于大规模的 RFID 系统, 所以该协议还需要在相应方面继续完善和改进.

参考文献

1 Juels A. RFID security and privacy: A research survey. Selected Areas in Communications, IEEE Journal on, 2006, 24(2): 381–394.

2 Song B, Mitchell CJ. RFID authentication protocol for low-cost tags. Proc. of the first ACM conference on Wireless network security. ACM. 2008. 140–147.

3 van Deursen T, Radomirovic S. Attacks on RFID Protocols. IACR Cryptology ePrint Archive, 2008: 310.

4 van Deursen T, Radomirovic S. Security of an RFID protocol for supply chains. e-Business Engineering, 2008. ICEBE’08. IEEE International Conference on. IEEE. 2008. 568–573.

5 Van Deursen T, Mauw S, Radomirović S. Untraceability of RFID protocols. Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks. Springer Berlin Heidelberg. 2008. 1–15.

6 van Deursen T, Mauw S, Radomirović S, et al. Secure ownership and ownership transfer in RFID systems. Computer Security–ESORICS 2009. Springer Berlin Heidelberg. 2009. 637–654.

7 Avoine G. Adversarial model for radio frequency identification. IACR Cryptology ePrint Archive,, 2005: 49.

8 Vaudenay S. On privacy models for RFID. Advances in Cryptology–Asiacrypt 2007. Springer Berlin Heidelberg. 2007. 68–87.

9 Ng CY, Susilo W, Mu Y, et al. RFID privacy models revisited. Computer Security-ESORICS 2008. Springer Berlin Heidelberg. 2008. 251–266.

10 Juels A, Weis SA. Defining strong privacy for RFID. ACM Transactions on Information and System Security (TISSEC), 2009, 13(1): 7–19.

11 Wolkerstorfer J. Is elliptic-curve cryptography suitable to secure RFID tags. Workshop on RFID and Lightweight Cryptography. Graz-August. 2005.

12 Batina L, Guajardo J, Kerins T, et al. An Elliptic Curve Processor Suitable For RFID-Tags. IACR Cryptology ePrint Archive, 2006,14(2): 206–227.

13 Lee YK, Sakiyama K, Batina L, et al. Elliptic-curve-based security processor for RFID. Computers, IEEE Transactions on, 2008, 57(11): 1514–1527.

14 Fan J, Verbauwhede I. Hyperelliptic curve processor for RFID tags. Workshop on RFID Security (RFIDsec). 2009. 129–139.

15 Martínez S, Valls M, Roig C, et al. A secure elliptic curve-based RFID protocol. Journal of Computer Science and Technology, 2009, 24(2): 309–318.